The Josai Journal of Business Administration (2025), Vol. 21, No. 1, 73−91
©2025, Josai University

Governing under Cyber Uncertainty:

Executive Decision-Making from the IT Boom to the AI Era (1990s–2020s)

Teruyoshi ADACHI, Shunichi TSUJI, Chisako TSUJI

Abstract

Digitalisation has created a paradox in executive decision-making: the very technologies that enable faster, data-driven management have also increased uncertainty through escalating cyber risks across integrated supply chains and software ecosystems.

In response, we contend that cyberresilient management has become a strategic imperative. Our framework prioritises cyber risk at the executive level, embeds identity-centred controls, strengthens third-party oversight, and cultivates an organisation-wide security culture. Coupled with clear performance measures (e.g., time to detect, contain, and recover), this integrated approach supports rapid innovation while preserving trust, rearchitects approvals for real-time action, institutionalises intelligence-led operations, and positions security and privacy as market differentiators. It offers practical guidance for reconciling growth with protection in an era where uncertainty is structural rather than episodic.

Keywords: Executive decision-making, Digital transformation, Enterprise risk management (ERM), Cybersecurity governance, Supply chain security, ERP integration

1. Introduction: The Paradox of Rationalisation and Uncertainty in Executive Decision-Making

P. F. Drucker noted in the first edition of his 1960 book, *Decision-Making for Innovation in Management,* that research on the basic themes of management and managers began during the decade of 1910−1920, citing works such as F. Taylor's *The Principles of Scientific Management*, J. A. Schumpeter's *The Theory of Economic Development*, and W. Rathenau's *The Social Role of the Company* as representative examples. He further observed that as of 1960, nothing was yet understood about top management, and any study in that area fell into one of two streams: either following Rathenau's line of examining the social responsibility of the firm, or Schumpeter's line focusing on the entrepreneurial role (Japan Management Association [1960], pp. 185−190). Given this situation, Drucker—at a time when managerial decision-making had not been fully discussed—set out from three approaches what knowledge and abilities a manager needs to lead a business to success.

The book repeatedly underscores the entrepreneurial function of the manager. According to Drucker, innovation is indispensable for modern companies that are required to create change, and producing such innovation is the entrepreneurial function of management; in other words, the function of the entrepreneur is "to create risk and to bear risk." Moreover, the capacity to perform this entrepreneurial function is cultivated "not by eliminating or minimising risk, but by attempting an even greater risk" (Japan Management Association [1960], p. 115). Drucker expected of contemporary executives "not to remove risk, and not to minimise risk,

but to enable the company to take on greater risk" (Japan Management Association [1960], p. 195).

Drucker's concept of the entrepreneurial function becomes more multifaceted and complex as a company grows and its internal and external environments change. In firms that start as micro-enterprises and grow into large corporations, when the baton passes from the founder to the next generation, the change in the entrepreneurial function required of the executive becomes apparent, and they are compelled to respond to it. If they neglect to adapt, the company will not achieve further growth.

Approximately 65 years have passed since Drucker wrote *Decision-Making for Innovation in Management*, and in that time research on managerial decision-making has steadily accumulated. In 1938, Chester Barnard, in *The Functions of the Executive*, set forth fundamental theories of organisations and leadership, and building on Barnard's achievements, Herbert Simon in 1947 examined decision-making and execution processes in organisations (1). It was not until the 1950s, however, that many researchers began to investigate decision-making from a variety of approaches, and this research took off in earnest from the 1960s onward.

Simon analysed organisations through the lens of decision-making behaviour, and his decades of contributions were recognised with the Nobel Prize in Economic Sciences in 1978. This recognition sparked heightened interest in decision-making processes within organisations. Then, in 1974, Daniel Kahneman - a pioneer of behavioural economics - together with Amos Tversky proposed *prospect theory* to describe how people make decisions under uncertainty, and Kahneman later received the Nobel Prize in 2002. This honour brought increased attention to discussions linking behavioural economics and decision-making. Thanks to these scholarly contributions, research on decision-making by executives and organisations today spans industries from agriculture to healthcare, and encompasses not only large corporations but also small and medium-sized enterprises. Moreover, active debate is underway on analytical methods to support decision-making, such as management accounting systems and business intelligence (2).

Simon once pointed out that considerations of management had been "*superficial, oversimplified, and lacking in realism. They were too narrowly confined to the formal mechanisms of authority, and failed to incorporate the influence of other, equally important, modes of organisational behavior*" (Simon [2009], p. 64). He argued that "*to establish a consistent and useful management theory, a new approach is necessary*" (Simon [2009], p. 497). Accordingly, he sought to view the business management process from the perspective of decision-making, in an attempt to explain management scientifically. Following Simon's perspective, research on the decision-making of executives and organisations can be regarded as a central theme of management science.

Against this backdrop, this paper looks back over roughly four decades—from the 1990s through the 2020s—during which advances in information technology profoundly altered the business environment. It organises the characteristics of digital technologies and cybersecurity phenomena relevant to executive decision-making into four periods. It examines, through representative cases and in historical context, how these developments have reshaped decisions at the top. Improvements in digital technology have enabled top management to access higher-quality information, yet exposure to cyber risks has simultaneously tightened the constraints of bounded rationality. Even so, appropriate executive choices can build a cyber-resilient governance structure that fosters entrepreneurial, forward-leaning risk-taking. Accordingly, this paper aims to articulate the strategic functions of top management under conditions of cyber risk.

2. The 1990s - Data Integration and the Birth of a Rationality-Vulnerability Paradox

2.1 Networked Supply Chains and Early IT Integration

The 1990s marked a turning point in corporate strategy, defined by unprecedented integration of operations and information flows on a global scale. As companies expanded their supply chains across borders, they turned to emerging digital technologies to coordinate far-flung activities in real time. The proliferation of personal computers, client-server architectures and the nascent internet provided a backbone for instant data sharing both within firms and with external partners. Ambitious projects were launched to link previously isolated functions (procurement, manufacturing, logistics, sales) into cohesive, information-rich networks. In effect, this decade witnessed the emergence of a more data-driven, 'rational' approach to executive decision-making that exemplified the offensive pursuit of efficiency and control—yet also planted the seeds of future vulnerability, as dependence on integrated systems created single points of failure.

Walmart offers a prominent example of the era's aggressive risk-taking enabled by data integration. By the early 1990s, Walmart was reinventing supply chain management through bold investments in information technology (Thomas Wailgum, 2007). The retailer was an early adopter of point-of-sale barcode scanning and even built a private satellite network to beam daily sales and inventory data from every store to headquarters. It also championed electronic data interchange (EDI), requiring suppliers to conduct routine transactions via standardised digital formats. This integration gave Walmart unprecedented transparency across its operations and supplier network. Many routine decisions - from reordering stock to scheduling deliveries - became automated and data-driven, freeing executives to focus on broader strategy. Notably, Walmart's leadership took a calculated risk by betting heavily on IT systems and mandating data connectivity with external partners - a move that more traditional competitors hesitated to emulate.

Walmart's integration extended beyond its own walls. In 1992, the company launched *Retail Link*, a pioneering collaboration with Procter & Gamble that directly connected Walmart's store-level sales data to P&G's production and distribution systems. The initiative instituted a replenishment regime that coordinated stock flows between the retailer and its principal supplier. Sales at Walmart triggered automated notices to P&G, prompting adjustments to production and replenishment without manual hand-offs. Within a few years, Retail Link was rolled out to thousands of suppliers. Decisions that once depended on monthly reports were now made using real-time data, vastly improving accuracy and responsiveness. At the same time, such deep interdependence introduced new governance challenges. By deploying information systems to exercise enterprise-wide oversight, Walmart substantially increased its leverage over suppliers. Vendors were, in effect, obliged to conform to the company's data specifications or face commercial marginalisation. Therefore, the production and distribution network became closely bound to Walmart's core platforms; any major outage or security incident affecting those systems could therefore have had significant knock-on effects across the wider network.

Similar transformations occurred in manufacturing. Toyota, for instance, digitised its renowned just-in-time *kanban* system during the 1990s, creating an electronic kanban that automatically signalled suppliers as soon as factory parts were consumed. By the end of the decade, Toyota had extended e-kanban to multiple plants, and other manufacturers were following suit. These efforts showed that the principle of data-integrated, rational deci-

sion-making was not confined to the retail sector. Across industries, executives began to rely on live digital signals rather than periodic manual reports, enabling leaner operations and more agile strategic adjustments.

2.2 Enterprise Resource Planning and Data-Driven Decisions

In parallel with supply chain innovations, large firms rapidly embraced enterprise resource planning (ERP) systems in the 1990s to integrate internal information and support executive decisions. By linking formerly siloed processes, ERP provided management with a holistic, real-time view of the entire enterprise. A CEO in the mid-1990s could, in principle, use an ERP dashboard to review yesterday's sales, today's production output and current inventory across all regions - an unprecedented level of synoptic insight and a single source of truth for decision-making. This comprehensive visibility enabled more rational, fact-based management daily, as critical information was no longer confined to departmental silos.

Empirical studies have shown that ERP adoption improves managerial speed and information consistency, enabling executives to act on unified, real-time data across the enterprise (Davenport, 1998). At the same time, the drive for integration revealed a paradox of control versus vulnerability. On one hand, unified platforms enabled the head office to impose common standards and tighten oversight, whilst accountability for day-to-day execution remained distributed across the organisation.

On the other hand, firms became deeply dependent on these complex platforms, which introduced new points of failure. ERP projects were notoriously expensive and risky. Such cautionary cases illustrated that the very systems granting managers greater control and rationality could, if mismanaged, wreak enormous damage.

These systems accelerated decision cycles and institutionalised evidence-based management, replacing intuition with data-driven judgement. A new ethos took root in many boardrooms: decisions large and small had to be justified with facts ("let's check what the data shows") rather than by precedent alone.

Second, organisational structures and cultures began to adapt to the information-rich environment. Integrated systems made departmental boundaries more transparent, as a change in one unit's data (for example, a new sales order) would instantly ripple through the plans of other units, such as production and shipping. Many firms reorganised to capitalise on this connectivity—creating cross-functional teams (for instance, supply chain management groups spanning procurement, manufacturing and distribution) to act on integrated information. IT leadership entered the C-suite, reinforcing the link between technology and strategy.

Third, the heavy reliance on IT integration introduced new risk considerations for top management. When business processes were digitised and tightly interlinked, a single system outage or software bug could bring operations to a standstill. For example, if an ERP system went down, it might halt not only accounting but also shop-floor production and order fulfilment that depended on the system's data. Consequently, business continuity planning and IT disaster recovery—once niche technical topics—became central to corporate risk management. The Y2K issue highlighted the dependency and vulnerability of integrated systems, prompting executives to recognise the risks associated with technology. As one retrospective noted, Y2K taught leaders that a single obscure "computer glitch" could jeopardise an entire enterprise, prompting enduring investment in IT risk management (McIndoe, 2009). It also demonstrated the value of cross-industry collaboration in tackling cyber vulnerabilities, foreshadowing the cooperative security approaches of later decades.

By the end of the 1990s, digital integration had fostered a paradox of control and vulnerability: executives gained rational oversight but became dependent on fragile systems. These

lessons set the stage for the 2000s, when firms would move to formalise cybersecurity governance and risk management to safeguard the foundations of their new data-driven decision-making capabilities.

3. The 2000s - From Rationalisation to Defensive Conformity: The Rise of Bounded Rationality

3.1 Compliance Regimes and Bounded Rationality

The early 2000s marked a decisive shift in corporate governance as a wave of high-profile failures and emerging cyber risks brought compliance to the forefront. In the United States, corporate scandals such as Enron and WorldCom led to the passage of the Sarbanes-Oxley Act of 2002, which, in Section 404 (Public Law 107−204, 2002), imposed stringent internal control requirements and heightened board-level accountability. Around the same time, new data protection laws signalled that cybersecurity could no longer be ignored: California's SB 1386 (2002) introduced the first mandatory data breach notifications, and Japan's Financial Instruments and Exchange Act of 2006 (colloquially "J-SOX") extended similar internal control mandates to Japanese firms. By the mid-2000s, virtually every primary jurisdiction had strengthened its regulatory stance on corporate IT risk, from state breach disclosure laws in the U.S. to the establishment of bodies like the European Network and Information Security Agency (ENISA) in the EU, making compliance with security and privacy norms a baseline expectation for doing business. Collectively, these interventions compelled executives to view cybersecurity not as a technical afterthought, but as a core aspect of governance and due diligence. Firms that suffered incidents now faced not only reputational damage but also legal penalties and intense scrutiny —a stark change from the more permissive environment of the 1990s.

This new compliance-driven climate introduced both discipline and dilemmas into executive decision-making, narrowing rationality by forcing leaders to equate regulatory conformity with security—an archetype of bounded rationality under defensive pressure. On one hand, the push for rationalisation of risk management through formal controls promised more systematic oversight. On the other hand, the growing burden of compliance began to encroach on managerial flexibility. Executives struggled to balance innovation, cost, and control under these constraints. They were now accountable for preventing security lapses, yet the prescribed solutions - detailed checklists of controls, audits, and certifications - often left little room for manoeuvre beyond "ticking the boxes." In effect, the proliferation of standards and regulations bound the rationality of decision-makers: faced with complex and evolving cyber threats, leaders gravitated towards the tangible certainty of compliance metrics as proxies for security. Resources were funnelled into meeting external mandates and passing audits, sometimes at the expense of more innovative or strategic investments in security. A cautious, defensive posture prevailed, as many firms sought to avoid fines and liability above all else.

One notable visible outcome of this era was the emergence of dedicated security governance roles, particularly the Chief Information Security Officer (CISO). By the mid-2000s, large organisations were appointing CISOs to bring cybersecurity into the C-suite. However, these early CISOs were primarily tasked with ensuring regulatory compliance above all else. Their success was measured by whether the company "passed audits and met legal requirements", underscoring how security efforts were channelled into a compliance-centric mould. In principle, better reporting and internal controls improved oversight; in practice, they also reinforced a mindset of avoiding downside risk rather than pursuing strategic upside. Thus, even as cybersecurity gained prominence in executive circles, it was often approached within a

narrow frame of bounded rationality - constrained by what could be justified to auditors and regulators, as well as by the finite cognitive bandwidth required to address the myriad new technical perils.

3.2 CardSystems Solutions: Compliance Pressure and Third-Party Risk

A vivid example of the decade's compliance-focused paradigm is the 2005 breach of CardSystems Solutions, a payment card processing company. In the 2005 incident at CardSystems, attackers obtained unauthorised access to around 40 million paymentcard records. Subsequent investigations identified serious weaknesses in the firm's security practices—among them missed patching and the improper retention of sensitive data—which, in combination, created conditions that made compromise more likely. The incident was a watershed moment that exposed how a single weak link in a network of business relationships could imperil numerous other companies - even industry giants were only as secure as their least secure partner in the transaction chain.

Crucially, the CardSystems breach coincided with the roll-out of the Payment Card Industry Data Security Standard (PCI DSS) in 2004 - a unified set of technical controls and audit requirements imposed on any organisation handling cardholder data. In the wake of the breach, the industry's response illustrated the defensive, compliance-oriented mindset of the time. Visa and Mastercard had set mid-2005 as the compliance date for processors under PCI DSS, a requirement that CardSystems conspicuously failed to meet. Once the breach became public, CardSystems was swiftly subjected to sanctions. This outcome sent a stark message to executives everywhere - that adherence to cybersecurity mandates was now a prerequisite for survival, not merely a box-ticking exercise. Firms rushed to verify that both they and their suppliers were in full compliance with PCI DSS and other applicable standards, lest they share CardSystems's fate.

The CardSystems saga typified how compliance pressure shaped corporate behaviour. Under the threat of legal liability and business sanctions, organisations prioritised measures that would satisfy regulators and industry overseers. Boards demanded assurances that "it can't happen here," often in the form of compliance certificates or third-party audit reports. In retrospect, this reliance on compliance as a safety net was itself a symptom of bounded rationality. Because executives could not possibly scrutinise every technical detail of operations or every partner's security from first principles, they leaned on prescribed frameworks (like PCI DSS) as a rational shortcut. These frameworks provided clear, if limited, guidance on what to do - such as installing firewalls, encrypting data, and conducting regular audits - which simplified decision-making in the face of uncertainty. However, as CardSystems demonstrated, nominal or delayed compliance alone could not guarantee actual security. The firm may have intended to get certified (and was reportedly given a grace period to do so), but real attackers exploited the latent gaps in the interim. The paradox was evident: executives had more guidelines than ever on how to protect their organisations, yet they often felt less free to act creatively, hemmed in by the need to demonstrably conform to external expectations. The defensive posture induced by compliance requirements, while prudent, often encouraged a reactive mentality - addressing known checklist items - rather than fostering a forward-looking strategy to anticipate future threats.

3.3 Microsoft's SDL: Proactive Adaptation and Resilience

Toward the latter half of the decade, a few organisations began to chart a different course, showing that compliance need not be the ceiling of their security ambition. The most influential case was Microsoft's introduction of its Security Development Lifecycle (SDL), which

represented a proactive, strategic adaptation to the cyber risk environment. In the early 2000s, Microsoft found itself at the epicentre of several cybersecurity crises: worms like Code Red (2001) and SQL Slammer (2003) had ravaged its Windows systems worldwide, exposing the fragility of software that had been developed with little built-in security. Rather than responding with piecemeal fixes or waiting for regulatory directives, Microsoft's top management took the unusual step of voluntarily overhauling the company's approach to product security. In January 2002, Bill Gates issued a landmark company-wide memo calling for "Trustworthy Computing" - essentially mandating that security and privacy become central to design, even if it meant delaying product releases. In early 2002, Microsoft paused feature development across its major product lines and enrolled thousands of engineers in secure coding training. By 2004, the company had institutionalised the SDL as a formal part of its engineering process, requiring every software project to incorporate threat modelling, code reviews, penetration testing, and secure configuration guidelines.

This initiative went well beyond any compliance requirement of the time - indeed, no law or regulation compelled Microsoft to adopt such stringent development protocols. The SDL was a voluntary strategic investment, born out of executive recognition that the company's future competitiveness depended on resilience. Early results validated this approach: the frequency and severity of vulnerabilities in Microsoft's products noticeably declined in subsequent releases. Just as importantly, Microsoft's leadership framed these security improvements as a selling point. The company publicly evangelised its SDL practices and touted the enhanced security of products like Windows 7 (released in 2009) as a competitive advantage. In doing so, Microsoft demonstrated that robust cybersecurity could be transformed from a mere compliance obligation into a market differentiator. This attribute builds customer trust and protects the bottom line.

Microsoft's SDL exemplified a turning point in executive mindset. Instead of reacting to external rules or waiting to be shaken into action by the next crisis, the company's executives chose to get ahead of the curve, integrating security into innovation. This shift can be seen as an escape from the bounded rationality that plagued others in the 2000s. Whereas many firms were content to meet the letter of compliance, Microsoft redefined the problem on its own terms: secure products would enable sustainable growth and fewer firefights, which in turn would save costs (by reducing emergency patches) and safeguard the firm's reputation. In essence, the SDL initiative replaced a reactive, checklist-driven mentality with a resilient design philosophy. It offered a blueprint for leveraging cybersecurity strategically, rather than merely tactically. Notably, the rest of the industry took notice. Other software companies and enterprises began emulating elements of the SDL, and the phrase "secure by design" entered the management lexicon as an aspirational goal. What Microsoft illustrated was that top management could align security with core business objectives - using it to enable reliability, customer confidence, and even agility - instead of viewing security as a compliance cost or a constraint on innovation.

In summary, the 2000s were a decade defined by the rise of compliance in cyber risk management and the attendant constraints on executive decision-making. Under intensifying regulatory oversight, companies adopted more formal and standardised defences, which undoubtedly professionalised their risk management but also often limited their perspective to what was mandated. This era's central paradox was that executives gained more guidance than ever on how to manage cyber risks. Yet, they often felt less free to act creatively, hemmed in by the need to demonstrably conform to external expectations. Still, by the decade's end, forward-thinking leaders had begun to glimpse a path beyond this paradox. The case of Microsoft's SDL demonstrated that adaptability and innovation in security can flourish even under

compliance pressures - and that exceeding requirements could transform cybersecurity into a source of strategic resilience. This set the stage for the 2010s, when many organisations would more explicitly strive to integrate cybersecurity into digital transformation and competitive strategy, moving from a posture of mere compliance to one of active cyber-resilience and value creation.

4. The 2010s - Digital Transformation, Board-Level Accountability, and the Expansion of the Innovation-Risk Paradox

4.1 Cloud, Mobile, and the Rise of Zero Trust - A New Digital Infrastructure

The 2010s saw enterprises embark on ambitious digital transformation initiatives, rapidly adopting cloud computing and mobile connectivity to drive agility and new business models. Migrating IT systems to cloud platforms fundamentally altered corporate infrastructures, and with them, the locus of security responsibility. Cloud providers formalised a shared-responsibility model: the platform's security rests with the provider, while customers retain responsibility for controls over their data, applications, and identities within the service. In practice, this meant executives could no longer assume that outsourcing to the cloud absolved them of security duties - a misconfigured storage bucket or lax identity control by the client could still lead to catastrophe. At the same time, the ubiquity of smartphones and Bring Your Own Device (BYOD) practices extended corporate networks far beyond office walls. Employees accessed company data from personal devices and public Wi-Fi, dissolving the traditional network perimeter. The attack surface expanded dramatically, exposing firms to threats that were well outside the purview of conventional IT oversight. These technological shifts enabled unprecedented operational agility, yet they also intensified the paradox between offensive innovation and defensive caution—executives gained power to act faster, but lost certainty in predicting and controlling outcomes.

In response, a new security paradigm took hold: Zero Trust architecture. Zero Trust abandons the notion of a trusted internal network; rather, each request, user, and device is verified on a continual basis, treating the environment as effectively as if it had no fixed perimeter. For executives, this represented a significant shift in perspective. No longer could firms rely on bolting firewalls around a well-defined perimeter; security had to be embedded by design across cloud and mobile environments, with investments in identity management, encryption, and continuous monitoring. Boards of directors became involved in approving these new security strategies, for example, scrutinising which cloud vendors to trust and insisting on "never trust, always verify" policies enterprise-wide. In short, cloud computing and mobile connectivity redefined corporate IT and elevated cybersecurity from a back-office IT concern to a core strategic issue for the organisation. Executives now had to weigh the tremendous upsides of digital innovation against the new visibility of cyber risk at the board level. This heightened the paradox of the 2010s: while digital transformation offered offensive opportunities for growth and innovation, it simultaneously amplified defensive challenges and uncertainties, forcing leaders to navigate between agility and caution in their strategic decisions.

4.2 Target 2013 - A Watershed Cybersecurity Breach and its Fallout

A turning point in executive accountability arrived with the 2013 Target Corporation data breach, which vividly demonstrated that cybersecurity failures could escalate into boardroom crises. In that incident - a veritable *watershed* moment - attackers infiltrated Target via a small third-party vendor. They installed malware on point-of-sale systems, ultimately stealing credit and debit card data for 40 million customers. The breach sparked public outcry and dozens of

lawsuits, and in its aftermath, Target's Chief Executive Officer and Chief Information Officer were forced to resign in early 2014. This was one of the first cases in which a Fortune 500 CEO lost their position primarily due to a cyber incident, sending a stark message across industries: a lapse in cybersecurity could cost top leadership their jobs. Target's board, facing shareholder anger and reputational damage, took an active role in the response and remediation. More broadly, the episode set a precedent that reverberated in boardrooms elsewhere. Directors began explicitly asking management, "What are we doing to ensure we're not the next Target?". By the mid-2010s, cyber risk had climbed sharply up the corporate agenda - often appearing as a priority item in quarterly board meetings. The Target breach thus crystallised a new reality: accountability for cyber governance had reached the highest levels of the organisation. In governance terms, this meant boards started treating cybersecurity as part of their fiduciary duty, even examining whether oversight failures might constitute negligence. The paradox of the decade was on full display - firms eager to embrace digital retail and data-driven marketing (offensive innovation) now found that a single security oversight (defensive lapse) could trigger leadership upheaval and intensive risk aversion virtually overnight.

4.3 Equifax 2017 - Data Compromise and the Strategic Reckoning

Another emblematic case underscoring executive accountability was the 2017 Equifax breach, one of the most consequential data breaches of the decade. In this incident, attackers exploited an unpatched web server vulnerability to exfiltrate personal records, for approximately 147 million individuals —nearly half of the U.S. population. The scale and sensitivity of the stolen data, coming from a credit bureau entrusted with safeguarding consumer information, made the breach front-page news globally. Equifax's CEO, CIO, and Chief Security Officer all resigned or retired in the aftermath, as the company scrambled to rebuild trust. It became clear that boards would demand executive heads roll when preventable security lapses led to such massive failures. The high-profile scrutiny that followed reinforced that cyber incidents had graduated from technical headaches to matters of public accountability. Crucially, the Equifax case also catalysed regulatory change. Within months, the European Union's landmark General Data Protection Regulation (GDPR) took effect in 2018, imposing penalties of up to 4% of a company's global revenue for mishandling personal data. While GDPR had been years in development, the narrative surrounding the Equifax debacle (along with earlier significant breaches such as Yahoo's) provided timely justification for stricter data protection regimes. For corporate executives around the world, GDPR proved a game-changer: suddenly, cybersecurity and privacy compliance carried direct financial consequences and legal liabilities at the strategic level. Firms worldwide - not just in Europe - invested heavily to harden their data governance and security controls, often overhauling how they stored and managed sensitive information. Many CEOs had to personally certify to their boards that their organisations were "GDPR-ready," and companies appointed Data Protection Officers and expanded CISO authority, recognising that regulators could hold the leadership itself accountable for lapses. In the United States, regulators likewise sharpened their stance. In 2018, the Securities and Exchange Commission (SEC) issued guidance requiring public companies to disclose material cyber risks and incidents. It urged boards to ensure they had cybersecurity expertise overseeing these matters. State-level regulations, such as New York's 2017 cybersecurity rule for financial institutions, added further teeth to the regulations. By the late 2010s, it had become common for boards to form dedicated cybersecurity committees and to expect regular cyber risk reports from management. In some organisations, executive compensation was even tied to security outcomes - for example, incorporating cyber incident metrics into CEOs' performance evaluations. The Equifax saga thus exemplified how a major breach could provoke

not only a crisis of leadership within a firm but also a broader strategic reckoning, industry practices, laws, and governance norms all shifted to treat cyber risk as a central business issue rather than a peripheral IT problem.

Notably, the fates of Target and Equifax underscored a typical lesson. In both cases, cyber insecurity led to rapid leadership turnover and legal action, indelibly embedding cybersecurity into the highest echelons of corporate governance. Top executives could no longer plead ignorance or hide behind technical teams; the expectation was set that they must actively govern cyber risk or face severe personal and organisational consequences. Through these examples, the decade's core paradox intensified: companies had to pursue digital innovation to stay competitive, yet any misstep in managing the attendant cyber risks could trigger disastrous, board-level fallout.

4.4 Balancing Innovation and Risk - The Executive's New Mandate

By the end of the 2010s, it was evident that cybersecurity had evolved from a niche concern into a strategic pillar of executive decision-making. No longer was cyber risk management delegated wholly to IT departments or compliance staff; it had become a "CEO issue", implicating customer trust, business continuity, and corporate reputation at the highest level. Chief executives increasingly emerged as visible champions of cybersecurity culture, setting the tone from the top and insisting that security and privacy be woven into every facet of the business. This leadership stance was necessary to reconcile the decade's defining tension between offensive innovation and defensive rationality. On the one hand, executives were under pressure to leverage new digital technologies, including cloud computing, mobile technology, big data, and automation, to drive growth and agile innovation. On the other hand, the very same digital expansion introduced complexities and threats that demanded prudent risk management and sometimes caution, given the limits of information and foresight (the essence of bounded rationality in decision-making). The strategic challenge for top management was therefore to navigate this paradox, enabling the organisation to "take on greater risk" through innovation, in Drucker's terms, while simultaneously controlling that risk to avoid catastrophe.

Leading organisations addressed this challenge by fundamentally integrating cybersecurity into their strategy and operations. Rather than viewing security as an impediment to innovation, they treated it as a prerequisite for sustainable innovation. By the late 2010s, many firms had adopted a "secure-by-design" or "secure innovation" mindset from project inception through execution. One concrete manifestation was the rise of DevSecOps - development practices that embed security checks and testing into the rapid software release cycles of the digital era. Executives championed DevSecOps because it promised to reduce the trade-off between speed and safety, allowing development teams to deploy new features at high velocity *without* leaving glaring vulnerabilities unchecked. In other words, businesses have learned to build resilience and security into their digital products and services from the ground up, thereby mitigating the bounded-rationality problem of unforeseen risks by instituting rigorous processes and oversight as part of their innovation. Some digitally native companies have even demonstrated that, with such practices, they can confidently push code updates dozens of times per day, with security serving as an in-built quality metric. The broader outcome was that a strong cybersecurity capability came to be seen as a source of competitive advantage. Corporate leaders realised that maintaining robust cyber defences and incident response readiness was essential to preserving the trust of customers, partners, and regulators - and that this trust, in turn, enabled the firm to pursue digital opportunities more boldly than less secure rivals. Indeed, a perspective emerged that effective cyber risk management could enable innovation: a company well-protected against threats could venture into new digital services or da-

ta-driven business models with greater confidence, whereas a less secure competitor might hesitate out of fear of breaches. By 2020, the most forward-looking enterprises had begun to convert cyber risk from a purely defensive concern into an opportunity to differentiate and excel. Scholars later termed this integrated approach "cyber-resilient management," which combines executive accountability, resilience by design, and converting risk into opportunity as a formula for sustained innovation and growth.

In summary, the 2010s concluded with a profound transformation in how top managers approached digital risk. Cybersecurity was now firmly entrenched in corporate strategy and governance, and the CEO's mandate had expanded to include active leadership in cyber risk management and crisis preparedness. Companies that successfully balanced the twin demands of offensive innovation and defensive vigilance found that strong cyber governance empowered their strategic ambitions rather than hindered them. This evolution set the stage for the 2020s, where even more complex challenges - from AI-driven threats to software supply chain vulnerabilities - would demand an even higher level of cyber resilience and strategic foresight from executives. The lessons of the 2010s - that digital trust and innovation are two sides of the same coin, and that executive decision-makers must continuously reconcile opportunity with risk - became the guiding principles for entering the new decade.

5. The 2020s - Complexity, AI, and the Quest for Cyber-Resilient Governance

5.1 Unprecedented Complexity and Bounded Rationality in Decision-Making

The 2020s have ushered in an era of unprecedented digital complexity. Organisations now rely on vast digital supply chains comprising software vendors, cloud services, and open-source components. This intricate ecosystem is so intertwined that no executive can fully comprehend its scope at any given time. Simultaneously, the rapid proliferation of AI-powered systems and automation has further obscured visibility. Decisions once made by humans are increasingly driven by algorithms and machine learning models, which, while efficient, often operate as opaque "black boxes" beyond intuitive understanding. As a result, top managers face an acute deepening of *bounded rationality* in their strategic choices. In Herbert Simon's classic formulation, executives can never attain perfect rationality due to cognitive limits and incomplete information; in the 2020s, this constraint has only intensified. The combined complexity of globally networked suppliers and AI-augmented processes means that complete information is effectively unattainable. Even the most diligent leadership teams struggle to obtain a comprehensive, real-time picture of their organisation's risk exposure. This gap between the need for swift, well-informed action and the inherent impossibility of knowing all pertinent facts defines the managerial context of the decade. In short, the decision-making environment of the 2020s amplifies Simon's insight that rationality is *context-bound and limited* - executives must make high-stakes choices under conditions of profound uncertainty and opacity.

Critically, this complexity has heightened the information asymmetry between attackers and defenders in cyberspace. Malicious actors thrive in the hidden interstices of digital supply chains, exploiting obscure software dependencies, third-party connections, and zero-day vulnerabilities that executives cannot reasonably track in their entirety. Meanwhile, well-intentioned innovations like AI can inadvertently compound the uncertainty. For example, generative AI tools now automatically produce code and configurations at scale, but may also introduce hidden flaws or biases. The same AI capabilities, accessible to attackers, enable highly sophisticated phishing and malware that evade human detection. Thus, technology that extends an organisation's capabilities can simultaneously enlarge its blind spots. In essence,

the very drivers of progress in this decade - hyper-connectivity, outsourcing, automation - have created a strategic predicament where knowledge is always partial and risk surfaces are diffuse. Leaders enter the 2020s cognisant that decisions must be made faster than ever, yet with less certainty than ever, requiring a new balance of vigilance and trust in the face of incomplete information.

5.2 The SolarWinds Attack: A Case of Hidden Dependencies and Opaque Risk

Nothing exemplified the dangers of this new complexity more starkly than the SolarWinds Orion supply chain attack, uncovered in December 2020. What appeared to be a routine software update for a widely used network management platform turned into a *Trojan horse* that compromised thousands of organisations. Attackers - later attributed to a nation-state's intelligence service - infiltrated SolarWinds' own development pipeline and surreptitiously inserted malicious code into an Orion software update. Around 18,000 customers deployed the compromised update, inadvertently creating persistent access paths into their systems. The intrusion provided adversaries with broad, persistent access to the networks of high-value targets, all under the guise of a trusted software patch. In effect, a single point of compromise in a third-party vendor cascaded into a systemic breach of unprecedented scope, an elegant exploitation of the implicit trust and opacity inherent in digital supply chains.

The SolarWinds breach went undetected for many months, a testament to the hidden and opaque nature of such risks. Throughout much of 2020, the attackers quietly surveilled and selectively exploited victim networks, while both SolarWinds and its clients remained oblivious. The campaign was ultimately exposed only when a cybersecurity firm (FireEye) noticed irregularities in its own environment, leading investigators back to the poisoned Orion update. By then, the damage was extensive: email systems, confidential data, and digital infrastructure across the U.S. government and global businesses had been stealthily accessed. Observers quickly labelled the incident one of the most far-reaching cyber-espionage campaigns in history, and a wake-up call regarding the fragility of modern supply chain defences. Public trust in the security of fundamental software plumbing was shaken, prompting urgent scrutiny of how such a compromise could have propagated so widely without being detected. Crucially, SolarWinds demonstrated that even *highly reputable, vetted vendors* could become unwitting conduits for attackers. In boardrooms worldwide, the uncomfortable question arose: *"What if the very tools we rely on are compromised at the source?"*.

From a governance perspective, the SolarWinds saga highlighted the limitations of traditional risk management frameworks in an era of complex and opaque dependencies. Before the attack, organisations tended to assess third-party risk through questionnaires, compliance checklists, and audits of vendor practices. Yet those controls presumed that vendors themselves exercised proper oversight internally. SolarWinds demonstrated how a sophisticated adversary could bypass even well-managed vendors by subverting their software build processes, a weakness that is primarily invisible to customers and not addressed by standard contracts or certifications. Indeed, a review by the U.S. Government Accountability Office noted that at the time of the breach, according to the U.S. Government Accountability Office, none of the twenty-three major federal agencies had, at that point, fully implemented the basic measures required for software supply-chain risk management. In other words, the public sector (much like private firms) was unprepared to govern the security of its suppliers' processes actively. Traditional controls proved to be reactive and superficial, as they failed to identify hidden failure points deep within the supply chain, creating a false sense of security. The Orion incident painfully exposed this gap. Even companies that adhered to prevailing best practices found themselves compromised, because those practices did not encompass verifying the integrity of

every software component coming from outside. Executives realised that their risk posture was only as strong as the weakest link in a sprawling chain of contractors, code libraries, and services - links over which they often had little visibility or control.

The immediate response to the SolarWinds incident underscored both the gravity of the threat and the difficulty of regaining control. Governments treated the breach as a national security emergency. In the United States, a Cyber Unified Coordination Group was convened to orchestrate a multi-agency response. In May 2021, the White House issued a sweeping Executive Order aimed at strengthening software supply chain security. Among other measures, this policy mandated that federal agencies require Software Bills of Materials (SBOMs) from vendors and implement stricter code integrity and vulnerability disclosure practices. These steps acknowledged that organisations can no longer operate on *assumed trust* - they must demand transparency into the components and pedigree of the software they deploy. In the industry, many enterprises likewise scrambled to harden their update and vendor management processes. Boards and CEOs pressed for evidence of suppliers' security (certifications, audit reports, penetration test results) beyond mere contractual assurances. Some firms instituted new internal controls, such as requiring a two-person review for any critical software update or testing patches in isolated sandboxes before deploying them enterprise-wide. Each of these reactions, however, came with a cost in agility. Slowing down updates or adding verification steps can mitigate risk, but it also delays improvements and fixes. Thus, SolarWinds not only highlighted a technical vulnerability, but also thrust onto the executive agenda a profound governance dilemma: how to reconcile the need for greater scrutiny and resilience with the imperative of speed in digital business.

5.3 The Decade's Core Paradox: Entrepreneurial Agility versus Defensive Resilience

The 2020s embody the culmination of the paradox that has defined executive decision-making since digitalisation began; leaders must act entrepreneurially in a hyper-connected world while accepting the limits of bounded rationality imposed by cyber uncertainty. Breaches and vulnerabilities of the SolarWinds kind demonstrated that even highly competent organisations could be caught unawares. In response, many executives adopted a mindset of "when, not if" regarding cyber incidents. This outlook acknowledges that preventive controls may fail; therefore, companies must excel at damage containment, recovery, and adaptation. Strategies like *Zero Trust* architecture moved from buzzword to baseline, urging firms to "never trust, always verify" every user, device, and software component as if an intruder might already be inside. At the same time, boards have come to expect robust business continuity and incident response plans that account for periodic disruptions. Leading enterprises invested heavily in resilience measures - from redundant cloud providers and offline backups to cyber insurance and tabletop breach simulations - all designed to absorb shocks and maintain critical operations even under attack.

Yet, these defensive investments form only one side of the paradox of the 2020s. Executives must also continue to drive offensive, entrepreneurial initiatives, pursuing digital transformation, innovation, and competitive advantage in a rapidly evolving market. Shareholders and stakeholders demand growth, which in practice means embracing new technologies (such as cloud, AI, and the Internet of Things), entering new digital ecosystems, and taking calculated risks in pursuit of opportunities. This creates an inherent tension between *agility* and *security*. On the one hand, firms need to remain agile - deploying new services, onboarding new partners, and updating systems rapidly to capitalise on business opportunities.

On the other hand, the ever-present threat of cyberattacks means that a single unmitigated risk can lead to devastating consequences if not adequately mitigated. The executive challenge

is to strike a balance between proactive risk-taking and prudent risk management. Prior research contends that leaders face a persistent tension: they must pursue strategic objectives through innovation whilst, at the same time, safeguarding critical assets through security. In parallel, they are expected to both reduce risk through controls and accept a measured degree of risk to enable progress. If they swing too far toward caution - locking down systems, adding layers of approval, or shying away from emerging tech - they may stifle the very innovation needed for long-term success. But if they err in the opposite direction, prioritising speed and growth while neglecting resilience, they court potentially existential threats from cyber disruptions. The paradox of this decade is that success requires *both* bold action *and* vigilant preparedness —a combination that is difficult to achieve with traditional, single-minded strategies.

Executive decision-makers in the 2020s thus find themselves walking a tightrope between opportunity and catastrophe. They must foster an organisational culture that *encourages innovation with a clear-eyed approach*. For example, a CEO pushing into cloud-based analytics must also champion rigorous cloud security reviews and staff training, lest a misconfiguration leak millions of customer records. A product team integrating a cutting-edge AI service should do so under the guidance of security architects who understand the risks associated with adversarial AI. These scenarios illustrate how modern leadership demands ambidexterity - the capacity to be agile and experimental, yet anchored by robust risk awareness and control. Recent high-profile incidents have reinforced that purely defensive postures are insufficient (since threats constantly evolve and some will penetrate), just as strictly offensive strategies are unsustainable (since unchecked risk eventually materialises). The *optimal stance* is a dynamic equilibrium: systems and processes that are flexible enough to adapt quickly to new conditions, yet also strong enough to withstand and recover from inevitable cyber shocks. Achieving this equilibrium is now a defining test of executive competence. Indeed, scholars and practitioners alike have observed that effective digital security governance requires engaging with these paradoxical tensions head-on and developing organisational routines to navigate them. In practice, that means integrating security thinking into every innovative venture (so that security is a built-in enabler, not an afterthought), and simultaneously, infusing the organisation's security and continuity planning with the creativity and agility traditionally reserved for growth initiatives.

5.4 Toward Cyber-Resilient Governance and Integrated Strategy

Confronting the complexity and paradox of the 2020s calls for a new mode of governance - one that deliberately blends agility with security at the highest levels of decision-making. Cyber-resilient governance has emerged as a unifying concept to describe this approach. At its core, cyber-resilient governance means structuring the organisation's oversight, processes, and culture such that it can innovate securely and secure innovation. Rather than viewing cybersecurity as a hindrance or a separate technical silo, leading firms now treat it as an integral component of strategic management. This involves explicit executive sponsorship of cyber resilience programs. These cross-functional governance bodies include both business and security leaders, and the elevation of metrics that gauge both opportunity and risk. For instance, boards increasingly review not only growth projections for a new digital product, but also its security readiness and the expected time to recover if it were compromised. Key performance indicators in top management dashboards may pair offensive goals (such as customer acquisition or deployment speed) with defensive ones (like mean time to detect incidents or the percentage of critical systems with up-to-date patches). By measuring and valuing both, organisations send a clear message: agility and protection must progress in tandem.

One practical manifestation of cyber-resilient management is the institutionalisation of continuous learning and adaptation in governance. The tumultuous early 2020s - marked by the SolarWinds attack, global ransomware outbreaks, and even a pandemic-driven surge in cybercrime have taught executives that static, plan-and-forget approaches are inadequate. In response, many companies have set up dedicated cyber risk committees or resilience steering groups at the board level. These groups regularly analyse intelligence on emerging threats and assess the implications for corporate strategy, ensuring that lessons from each incident (internal or external) are swiftly translated into improvements. Such governance mechanisms enable what might be called *strategic agility with safety nets*: the organisation can pivot or upscale digital initiatives quickly, confident that if a new threat arises, there is a process to recalibrate controls and responses without derailing overall progress. In tandem, regulatory developments are nudging companies in this direction. Regulatory regimes in the 2020s (from strengthened data protection laws to sector-specific cyber rules) increasingly demand both the proactive management of cyber risk and evidence of resilience planning. Executives, under scrutiny of regulators and investors, have even greater incentive to embed cybersecurity into corporate governance - not as a checkbox compliance matter, but as a dimension of fiduciary duty and strategic foresight. In addition, organisations are recognising the need for industry-wide collaboration on cyber resilience. Leading companies now participate in information-sharing alliances and public-private partnerships to collectively strengthen defences and respond to threats, reflecting the understanding that no single firm can manage cyber risk in isolation.

In summary, the journey through the 2020s has crystallised a vision of executive leadership that reconciles the entrepreneurial and the vigilant. This decade's defining lesson is that offence and defence in corporate strategy need not be in conflict but can be coherently unified. The SolarWinds incident and its aftermath underscored the importance of this unity: firms must maintain both the offensive capacity to drive growth through digital innovation and the *defensive* muscle to withstand and adapt to shocks. The old dichotomy between business strategy and IT risk management is dissolving. In its place, a more holistic model of governance is emerging - one in which cybersecurity serves as both a guardrail and a driver of value. Executives who embrace cyber-resilient management treat each new technology adoption as an opportunity to build competitive advantage *and* organisational robustness, seeing the two aims as mutually reinforcing. Under such governance, a firm can confidently navigate the volatile 2020s: it remains agile enough to seize emergent opportunities, yet resilient enough to survive the unforeseen adversities that are the price of digital ambition. This ambidextrous approach not only resolves the decade's paradox but also sets the stage for sustainable success in an era where the only certainty is the unpredictability of cyber risk.

6. Conclusion: Reconciling the Offensive and Defensive Functions of Executive Decision-Making

This paper has examined how digitalisation has both rationalised and paradoxically constrained executive decision-making, revealing how the tension between offensive innovation and defensive rationality culminates in the need for cyber-resilient management.

With respect to the importance of digitalisation and cybersecurity in corporate decision-making, this study has reviewed approximately forty years, from the 1990s to the 2020s, during which advances in information technology transformed the managerial environment. We organized the salient features of digital technologies and cybersecurity events affecting executive decisions into four periods, and, drawing on representative cases and regulatory developments, considered the current challenges and prospects for corporate management in light of

their historical evolution. Our scope encompassed significant corporate instances of cybersecurity, including Walmart, Toyota, CardSystems Solutions, Target, Equifax, and SolarWinds, as well as institutional changes such as SOX, J-SOX, and GDPR. Based on literature, documents, and case analyses, we synthesized each period's characteristic patterns and compared firms' responses and governance shifts from the perspectives of bounded rationality and resilience.

In the 1990s, efficiency gains and tighter control were achieved through the integration of IT. At the same time, new vulnerabilities also surfaced in the form of enterprise-wide effects when system failures or security incidents occurred. Through ERP rollouts and the Y2K issue, senior executives came to recognise the importance of managing IT risk. In the 2000s, amid corporate scandals and rising cyber risk, regulations such as SOX and JSOX were strengthened, and compliance-centered governance became mainstream. However, an overemphasis on formal compliance gave rise to a problem of bounded rationality, narrowing the scope for substantive safety and creative responses. From the 2010s onward, the widespread adoption of cloud and mobile technologies, as well as the emergence of Zero Trust, has made cybersecurity a core concern for top management. The Target and Equifax incidents demonstrated that cyber risk is directly linked to executive accountability and corporate strategy, accelerating a shift toward DevSecOps and cyber-resilient management. In the 2020s, dependence on diverse digital resources, including AI, automation and open source, has increased, making it challenging to maintain a synoptic view of the organisation. Our analysis of the SolarWinds incident highlighted the limitations of traditional risk management and underscored the need to enhance supply chain oversight and management.

From our analysis, it is clear that cybersecurity governance has developed while internalizing a paradox of efficiency and tighter control alongside the growth of vulnerability and risk. For corporate leaders to go forward, it is essential to advance cyber-resilient governance that assumes the inevitability of incidents and reconciles resilience with growth and innovation. At the board level, evaluating growth and security metrics in tandem and embedding a culture that balances agility and defensive capability are keys to sustained growth and safety.

It is evident from recent security incidents that cybersecurity has become an urgent managerial and organisational issue. In a recent case, Asahi Group Holdings disclosed on 25 September 2025 that a cyber incident, believed to be a ransomware attack against core systems, forced the simultaneous suspension of domestic order intake, shipping, and call centre operations. Observers have noted that the integration of information systems undertaken by many companies to improve efficiency can amplify the scope of cyber damage across entire supply chains and prolong recovery times. Reports have also indicated the possibility that personal information was leaked (Nihon Keizai Shimbun [2025b]). Given the breadth of the impact and the protracted restoration, it is reasonable to infer significant shortcomings in resilience functions, including backup practices, as well as in the operation and management of data. Harmonizing systems investment with security investment is a key responsibility of senior management, yet this incident underscores that even flagship Japanese corporations have not fully achieved that balance.

By contrast, the case in which Trial Holdings ("Trial") acquired all shares of Seiyu Co., Ltd. ("Seiyu") and made it a wholly owned subsidiary as of 1 July 2025 can be seen as a management strategy that leverages inhouse IT capabilities, including cybersecurity, as a driving force for M&A to expand the business and its marketing reach. The transaction was intended to realize synergies between Trial's technological capabilities and Seiyu's sales network and brand, with the initiative stemming from Trial's ownership of its own IT assets (Kabushiki Kaisha Trial Holdings [2025a]). Trial began in 1974 in Fukuoka as a recycling shop (adopting

its current corporate name in 1984), subsequently moved into personal computer sales and software development, and since the 1990s has expanded into the discount retail format. As a company, it launched software development before its supermarket business. It has focused on developing IT systems for distribution, often called "retail tech", ranging from POS systems to smart carts, cashier-less payment, AI and retail media. Today, as one of the pillars of the group, several subsidiaries run an in-house engineer-led "Retail AI" business (Kabushiki Kaisha Trial Holdings [2025b]). Section 2 of this paper examined Walmart's strategy of using IT as a growth engine. Walmart had entered a comprehensive business alliance with Seiyu in 2002 and made it a wholly owned subsidiary in 2008 (with Rakuten later joining management in 2021). In the present case, Trial, sometimes dubbed a "homegrown Walmart", is acquiring Seiyu with its in-house IT as the propulsive force. This suggests that Japanese firms have entered an era in which strategies on a par with Walmart's can be executed (Nihon Keizai Shimbun [2025a]).

In this paper, we have mapped the historical trajectory since the 1990s, in which advances in IT have driven the integration of supply chains and business processes, enabling data-driven decision-making by senior management while simultaneously exposing new vulnerabilities, such as system failures and cyber risks, alongside efficiency gains. Our next step is to focus on factors likely to influence forthcoming corporate management reforms, identifying, cataloguing, and analysing significant security cases from the perspectives of technology, management, and enforcement. Building on detailed case studies, we will continue our inquiry with a research plan that explores the potential to theorise using bounded rationality, extracts and examines the factors necessary for theory building, and considers the feasibility of a transaction-cost approach.

Bernstein points out that the English word "risk" derives from the Latin language, meaning "to dare," and thus "risk is not so much a fate as it is a choice" (Bernstein [1998], p. 23). Keeping legal and regulatory developments in view, the authors will continue to consider how the integration of cybersecurity management and decision-making processes can foster innovation by transforming risks into opportunities.

Author contributions: Teruyoshi ADACHI drafted Sections 2–5, Shunichi TSUJI drafted Section 6, Chisako TSUJI drafted Section 1.

Appendix: Major Developments by Period

Period	Technological and Societal Context	Representative Cases and Regulatory Milestones	Managerial and Decision-Making Implications
Pre-1980s (Theoretical Foundations)	Formative stage of management and decision-making theory; pre-digital environment.	H. A. Simon, *Administrative Behavior* (1947); D. Kahneman & A. Tversky's Prospect Theory (1974).	Established the conceptual bases of bounded rationality and risk-based decision-making, positioning decision processes at the core of management science.
1990s - Data Integration and Emerging Vulnerability	Rapid spread of ERP, the Internet, and EDI; early globalisation of data exchange.	Walmart's *Retail Link* (1992); Toyota's electronic *kanban*; Y2K issue (1999).	Decision-making became data-driven and accelerated, yet growing IT dependence created single points of failure. Integration brought both efficiency and systemic fragility.
2000s - From Rationalisation to Defensive Conformity	Intensified regulatory oversight following corporate and data scandals; emergence of compliance regimes.	Sarbanes-Oxley Act (2002); California SB 1386 (2002); J-SOX (2006); PCI DSS (2004); CardSystems breach (2005).	Compliance-oriented governance professionalised cyber risk management but constrained managerial flexibility. Rationality became bounded by audit-driven conformity.

Late 2000s - Proactive Adaptation and Security by Design	Rising awareness of software vulnerabilities and secure development practices.	Microsoft's "Trustworthy Computing" memo (2002); institutionalisation of the Security Development Lifecycle (2004).	Shift from reactive compliance to strategic resilience; security reframed as a competitive advantage and a driver of reliability.
2010s - Digital Transformation and Board-Level Accountability	Widespread adoption of cloud and mobile technologies; Zero Trust architecture; new data protection regimes.	Target breach (2013); Equifax breach (2017); EU GDPR enforcement (2018); SEC cybersecurity disclosure guidance (2018).	Cybersecurity elevated to a board responsibility. Executive decision-making expanded to integrate cyber risk, governance, and innovation (DevSecOps, "secure by design").
2020s - Complexity, AI, and Cyber-Resilient Governance	Proliferation of AI, automation, and cloud supply chains; rising opacity of dependencies.	SolarWinds attack (2020); U.S. Executive Order on supply chain security (2021); Software Bill of Materials (SBOM) requirements; Osaka General Medical Centre ransomware (2022); Asahi Group Holdings incident (2025).	Decision-making increasingly constrained by complexity and uncertainty. Boards prioritise resilience, transparency, and real-time intelligence to counter bounded rationality.
Towards the 2030s - Institutionalising Cyber-Resilient Management	Convergence of digital transformation, legacy renewal, and legislative evolution.	Japan's "2025 Digital Cliff" report (METI, 2018); ongoing debates on Active Cyber Defence legislation.	Corporate governance expected to reconcile innovation with defence, embedding automation and intelligence-led oversight into executive decision-making architectures.

Notes:

(1) The first edition of *Administrative Behaviour* was published in 1947, and up to a fourth edition was subsequently released. For details, see Nobuo Takahashi [2008], "'Gentei sareta gourisei' wa doko ni: Keieigaku rinkou Simon (1947, 1957, 1976, 1997)" (*"Where is 'Bounded Rationality': A Management Seminar on Simon (1947, 1957, 1976, 1997)"*), *Akamon Management Review*, Vol. 7, No. 9 (September 2008), pp. 687−706.

(2) Today, research on decision-making is classified into several approaches - such as the organisational behaviour approach, the behavioural science approach, and the systems analysis approach - and many studies have been accumulated on the foundation of those earlier achievements.

References

Adachi, T. (2025). The new logic: How to think, decide, and win in the age of AI. Independently published.

Akerlof, G. A. (1970). The market for "lemons": Quality uncertainty and the market mechanism. Quarterly Journal of Economics, 84(3), 488−500.

Amazon Web Services. (2017). Shared Responsibility Model. Seattle, WA: Amazon Web Services.

Barnard, C. I. (1968). Keieisha no Yakuwari [The Functions of the Executive] (Y. Yamamoto et al., Trans., New ed.). Tokyo: Diamond, Inc. (Original work published 1938)

Bernstein, P. L. (1998). Risk: Kamigami heno Hangyaku [Against the Gods: The Remarkable Story of Risk] (M. Aoyama, Trans.). Tokyo: Nihon Keizai Shimbunsha. (Original work published 1996)

California State Legislature. (2002). Senate Bill 1386: Security Breach Information Act. Sacramento, CA: California State Legislature.

Davenport, T. H. (1998). Putting the enterprise into the enterprise system. Harvard Business Review, 76(4), 121−131.

How Wal-Mart lost its technology edge. (2007, 1 August). CIO. Retrieved from https://www.cio.com/article/274579/strategy-how-wal-mart-lost-its-technology-edge.html. (Accessed: 14 May 2025)

Japan Management Association (Ed.). (1978). Drucker Meicho Senshu (4): Keiei Kakushin e no Ishikettei [Drucker Selected Works, Vol. 4: Decision-Making for Innovation in Management]. Tokyo: Japan Management Association. (Original work by P. F. Drucker published 1960).

Japanese Diet. (2006). Financial Instruments and Exchange Act. Tokyo: Government of Japan.

Kabushiki Kaisha Toraiaru Horudingusu [Trial Holdings Co., Ltd.] (2025a). *Kabushiki Kaisha Seiyu no kabushiki no shutoku (kanzen kogaishaka) ni kansuru setsumei shiryo* (Explanatory Materials on the Acquisi-

tion of Shares of Seiyu Co., Ltd. [Making it a Wholly Owned Subsidiary]). 5 March 2025. Available at: https://pdf.irpocket.com/C141A/KHnJ/IzXg/IJDl.pdf. (Accessed: 14 May 2025)

Kabushiki Kaisha Toraiaru Horudingusu [Trial Holdings Co., Ltd.] (2025b). *Jigyo Naiyo* (Business Overview). Available at: https://trial-holdings.inc/business/#retail-ai. (Accessed: 14 May 2025)

Markus, M. L., & Tanis, C. (2000). The enterprise systems experience: From adoption to success. In R. W. Zmud (Ed.), Framing the domains of IT research: Glimpsing the future through the past (pp. 173−207). Cincinnati, OH: Pinnaflex.

McIndoe, B. (2009, 1 December). The decade of risk. Risk Management Magazine. Retrieved from http://www.rmmagazine.com/articles/article/2009/12/01/-the-decade-of-risk-. (Accessed: 14 May 2025)

Ministry of Economy, Trade and Industry (METI), Industrial Cybersecurity Study Group [2023] Final Report of the Study Group on Promoting Information Sharing on Damages Caused by Cyberattacks, 22 November. Available at: https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/cyber_attack/pdf/20231122_2.pdf. (Accessed: 14 May 2025)

Nihon Keizai Shimbun (2025a). *Seiyu henkaku, wasei Uorumaato saichosen—kouri sedai koutai wo utsusu* (Seiyu's Transformation and a "Japanmade Walmart" Tries Again: A Generational Shift in Retail). 8 March 2025. Available at: https://www.nikkei.com/article/DGXZQOCD090Y80Z00C25A2000000/. (Accessed: 14 May 2025)

Nihon Keizai Shimbun (2025b). *Asahi GHD, saibaa kougeki no eikyo tsuzuku* (Asahi GHD: Ongoing Effects of Cyberattack). 4 October 2025. Available at: https://www.nikkei.com/article/DGXZQOUC-024330S5A001C2000000/. (Accessed: 4 October 2025)

Public Law 107−204. (2002). Sarbanes-Oxley Act of 2002. Washington, DC: U.S. Government Printing Office.

Ttsuta, D. (2024). Overview and issues of cybersecurity legislation. Jurist, (1559), 34−40.〔蔦大輔「サイバーセキュリティ法制の概観と課題」有斐閣編『ジュリスト』有斐閣、2024 年 7 月〕

Simon, H. A. (2009). Keiei Koudou [Administrative Behavior] (T. Nimura et al., Trans., New ed.). Tokyo: Diamond, Inc. (Original work published 1947)

Toyota Motor Corporation. (n.d.). 75 years of Toyota: Production parts logistics. Retrieved from https://www.toyotaglobal.com/company/history_of_toyota/75years/data/automotive_business/production/logistics/production_parts/. (Accessed: 14 May 2025)

Tsuji, C., Adachi, T., & Tsuji, S. (2022). Measure for measurement: How to connect efficient cyber risk management with strategic decision-making. The Josai Journal of Business Administration, 18(1), 1−19.

Tsuji, C., Tsuji, S., & Adachi, T. (2023). To integrate or collaborate: Strategies for effective cyber risk management and cybersecurity. The Josai Journal of Business Administration, 19(1), 11−26.

Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. Science, 185(4157), 1124−1131.

U.S. Government Accountability Office. (2021, 22 April). SolarWinds cyberattack demands significant federal and private-sector response (infographic). Washington, DC: U.S. GAO. Retrieved from https://www.gao.gov/blog/solarwinds-cyberattack-demands-significant-federal-and-private-sector-response-infographic. (Accessed: 14 May 2025)